(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 122 932 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.08.2001 Bulletin 2001/32

(51) Int Cl.7: **H04L 29/06**

(21) Application number: **01102150.8**

(22) Date of filing: **01.02.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.02.2000 US 498093**

(71) Applicant: **Aladdin Knowledge Systems Ltd.**
Tel Aviv 67211 (IL)

(72) Inventors:
- **Margalit, Dany**
  Ramat Gan 52223 (IL)
- **Gruper, Shimon**
  Kiryat Haim 26307 (IL)

(74) Representative: **Modiano, Guido, Dr.-Ing. et al**
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
80469 München (DE)

(54) Protection of computer networks against malicious content

(57) A gateway including an input for receiving communications packets, an output for outputting communications packets generally in real time with respect to receipt thereof, a policy manager determining criteria for collection and inspection of a collection of packets and a packet collection agent receiving packets from the input in accordance with criteria established by the policy manager and including a content inspector inspecting the collection of packets in accordance with criteria established by the policy manager and being operative to prevent supply of at least one packet of a collection of packets to the output when the collection of packets includes undesirable content in accordance with the criteria established by the policy manager.

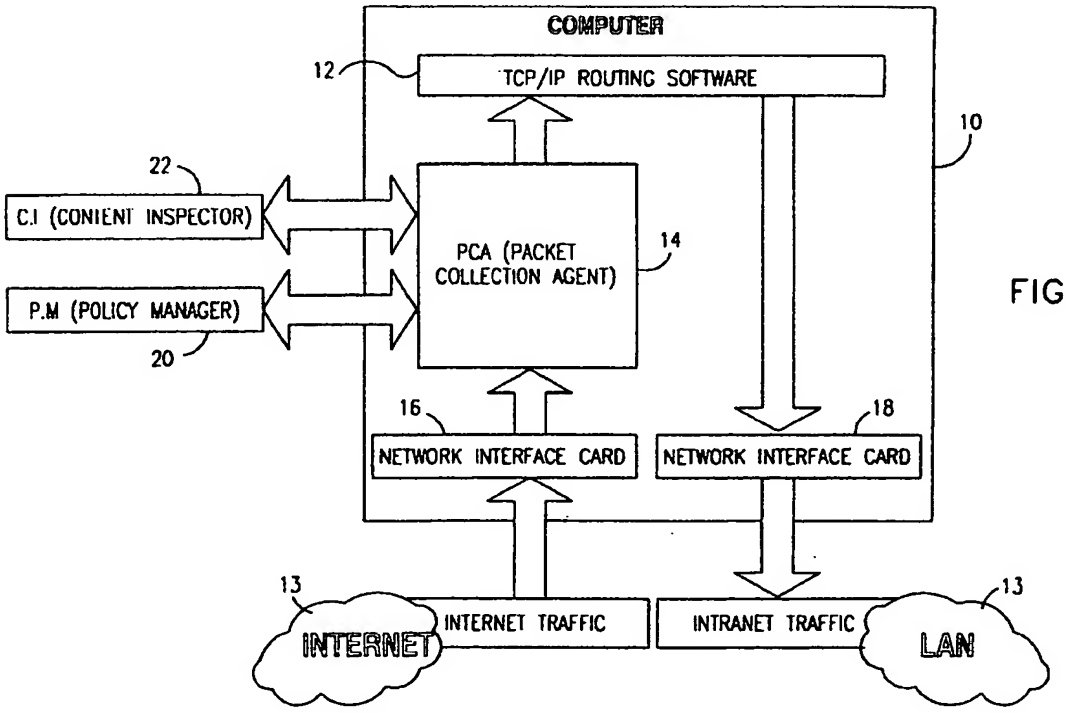


FIG. 1A

EP 1 122 932 A2

Description

FIELD OF THE INVENTION

[0001] The present invention relates to computer network communications generally and more particularly to apparatus and methods for providing security in computer network communications.

BACKGROUND OF THE INVENTION

[0002] There exist a large number of U.S. Patents which deal with security in computer network communications. The following U.S. Patents and the references cited therein are believed to represent the state of the art: 5,951,698; 5,918,008; 5,907,834; 5,892,904; 5,889,943; 5,881,151; 5,859,966; 5,854,916; 5,842,002; 5,832,208; 5,826,012; 5,822,517; 5,809,138; 5,802,277; 5,748,940; 5,684,875; 5,679,525; 5,675,711; 5,666,411; 5,657,473; 5,649,095; 5,623,600; 5,613,002; 5,537,540; 5,511,184; 5,111,163; 5,502,815; 5,485,575; 5,473,769; 5,452,442; 5,398,196; 5,359,659; 5,319,776.

[0003] Security in computer network communications deals with two general types of malicious content which may be communicated over a network to a computer: viruses and vandals. Viruses may be classified into a number of categories, such as file infectors, file system viruses, macro viruses and system/boot record infectors.

[0004] Vandals are distinguished from viruses in that whereas viruses require a user to execute a program in order to cause damage, vandals are auto-executable Internet applications and may cause immediate damage. Currently the following types of vandals are known: Java applets, ActiveX objects, scripts and cookies. Vandals may hide in various types of communicated content, including Email, web content, legitimate sites and file downloads.

[0005] It is known to employ proxy servers to detect and prevent receipt of malicious content by a computer. Use of proxy servers for this type of application is described inter alia in the aforesaid U.S. Patents 5,951,698; 5,889,943 & 5,623,600. The use of proxy servers for this purpose has a number of disadvantages including non-real time operation, generation of network bottlenecks, requiring special configuration of each desktop and relative ease of bypass by a user.

SUMMARY OF THE INVENTION

[0006] The present invention seeks to provide apparatus and a method for protection of computers against malicious content generally in real time and without requiring the use of a proxy server.

[0007] There is thus provided in accordance with a preferred embodiment of the present invention a gateway including an input for receiving communications packets, an output for outputting communications packets generally in real time with respect to receipt thereof, a policy manager determining criteria for collection and inspection of a collection of packets and a packet collection agent receiving packets from the input in accordance with criteria established by the policy manager and including a content inspector inspecting the collection of packets in accordance with criteria established by the policy manager and being operative to prevent supply of at least one packet of a collection of packets to the output when the collection of packets includes undesirable content in accordance with the criteria established by the policy manager.

[0008] There is also provided in accordance with a preferred embodiment of the present invention a method for protecting a computer from malicious content comprising the steps of:

determining criteria for collection and inspection of a collection of packets;
receiving packets from among the collection of packets in accordance with the criteria;
inspecting the packets in accordance with the criteria;
preventing output of at least one packet but not all packets of a collection of packets when the collection of packets includes undesirable content in accordance with the criteria; and
outputting packets other than the at least one packet generally in real time with respect to receipt thereof;

[0009] In accordance with a preferred embodiment of the present invention, the at least one packet is the last packet of a file.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1A is a simplified block diagram illustration of implementation of the invention in a firewall-type configuration for checking incoming Internet but not intranet traffic;
Fig. 1B is a simplified block diagram illustration of implementation of the invention for checking all incoming communications;
Fig. 2 is a simplified block diagram illustration of the use of multiple content inspectors by a single packet collection agent; and
Fig. 3 is a simplified flow chart illustrating operation of a packet collection agent in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0011] The present invention seeks to provide protection of a computer against malicious content without requiring the use of a proxy server.

[0012] Reference is now made to Fig. 1A, which is a simplified block diagram illustration of implementation of the invention in a firewall-type configuration for checking incoming Internet but not intranet traffic. As seen in Fig. 1A, there is provided a typical computer 10 in which resides conventional TCP/IP routing software 12. Computer 10 is typically connected to a network 13.

[0013] In accordance with a preferred embodiment of the present invention a packet collection agent (PCA) 14 is interposed between a network interface card (NIC) 16 which receives Internet traffic and the TCP/IP routing software 12. In this embodiment, a separate NIC 18 handles intranet traffic and does not have a PCA interfaced between it and the TCP/IP routing software 12.

[0014] In accordance with a preferred embodiment of the present invention, the PCA 14 interfaces with policy manager software 20, which determines collection criteria, i.e. which types of packets of which types of files are collected, and inspection criteria, i.e. which types of content in a file are not allowed to pass to or from network 13.

[0015] Based on the criteria established by the policy manager software 20, the PCA 14 operates content inspector software 22, which inspects the packets of a file which fits the criteria for collection and inspection. The content inspector software 22 operates based on criteria established by the policy manager software 20 and reports its inspection findings to the PCA 14. Alternatively, policy manager software 20 may be obviated. In such a case, the PCA 14 and the content inspector software are each programmed with suitable criteria.

[0016] In accordance with a preferred embodiment of the invention, the PCA 14 does not delay transmittal of most packets, even of files that require inspection. Rather, while transmitting all but typically the last packet in a file, it operates content inspector software 22 to inspect the contents of the file. If the contents are found to be acceptable, typically the last packet is released. If the contents of a file are not found to be acceptable by the criteria typically established by the policy manager software 20, at least one packet, typically the last packet, is not released, preventing activation of the unacceptable content by the computer.

[0017] Reference is now made to Fig. 1B, which illustrates implementation of the invention for checking all incoming communications along a network 28. In this illustrated embodiment, as seen in Fig. 1B, there is provided a typical computer 30 on which resides TCP/IP software 32. In accordance with a preferred embodiment of the present invention, a packet collection agent (PCA) 34 is interposed between a network interface card (NIC) 36, which receives Internet and intranet traffic, and the TCP/IP software 32.

[0018] In accordance with a preferred embodiment of the present invention, as in the embodiment of Fig. 1A, the PCA 34 interfaces with policy manager software 40, which determines collection criteria, i.e. which types of packets of which types of files are collected, and inspection criteria, i.e. which types of content in a file are not allowed to pass to the computer.

[0019] Based on the criteria typically established by the policy manager software 40, the PCA 34 operates content inspector software 42, which inspects the packets of a file which fits the criteria for collection and inspection. The content inspector software 42 operates typically based on criteria established by the policy manager software 40 and reports its inspection findings to the PCA 34.

[0020] In accordance with a preferred embodiment of the invention, the PCA 34 does not delay transmittal of most packets, even of files that require inspection. Rather while transmitting all but typically the last packet in a file, it operates content inspector software 42 to inspect the contents of the file. If the contents are found to be acceptable, typically the last packet is released. If the contents of a file are not found to be acceptable by the criteria typically established by the policy manager software 40, at least one packet, typically the last packet, is not released, preventing activation of the unacceptable content by the computer.

[0021] Reference is now made to Fig. 2, which is a simplified block diagram illustration of the use of multiple content inspectors by a single packet collection agent. As illustrated in Fig. 2, a single PCA 50 may interface with a single policy manager 52, which may, in certain embodiments be obviated, and with a plurality of content inspectors 54 simultaneously. This type of arrangement may be particularly useful for handling high traffic volumes.

[0022] Reference is now made to Fig. 3, which is a simplified flow chart illustrating operation of a PCA in accordance with a preferred embodiment of the present invention.

[0023] As seen in Fig. 3, upon receipt of a packet, if the packet is received in the context of an existing file and is not the last packet, the packet is simultaneously stored and released to its destination, generally in real time.

[0024] If the packet is the last packet in a file, the PCA typically obtains the inspection criteria from the policy manager and sends all of the packets in the file to a content inspector for inspection in accordance with the inspection policy typically established by the policy manager. If the file passes inspection, the last packet is released as well. If not, the last packet is not released.

[0025] If the packet is the first packet of a new file and thus is a control packet as opposed to a data packet, the PCA employs the collection criteria typically established by the policy manager to determine whether the file requires inspection. If not, the packet and all subse-

quent packets of that file are immediately released as they arrive. If the file is a type of file that is not permitted, no packets are released. If, however, the file is a type of file that requires inspection, the packet is immediately released and the subsequent packets are inspected.

[0026] It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of various features described hereinabove and in the drawings as well as modifications and variations thereof which would occur to a person of ordinary skill in the art upon reading the foregoing description and which are not in the prior art.

[0027] Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A gateway comprising:

   an input for receiving communications packets;
   an output for outputting communications packets generally in real time with respect to receipt thereof;
   a policy manager determining criteria for collection and inspection of a collection of packets;
   a packet collection agent receiving packets from said input in accordance with criteria established by said policy manager; and
   at least one content inspector operated by the packet collection agent and inspecting said collection of packets in accordance with criteria established by said policy manager,
   said packet collection agent being operative to prevent supply of at least one packet of a collection of packets to said output when said collection of packets includes undesirable content in accordance with said criteria established by said policy manager.

2. A gateway according to claim 1 and wherein said at least one packet is the last packet of a file.

3. A gateway according to claim 1 or claim 2 and wherein said policy manager determines criteria whereby not all files are inspected.

4. A gateway according to any of claims 1 to 3 and wherein said packet collection agent inspects all packets of files that are to be inspected.

5. A gateway according to any of claims 1 to 4 and wherein said packet collection agent operates plural content inspectors simultaneously.

6. A gateway according to any of claims 1 to 5 and wherein said policy manager determines criteria whereby some types of files are not released even without inspection by a content inspector.

7. A gateway according to any of claims 1 to 6 and wherein said packet collection agent operates on Internet but not on intranet traffic.

8. A gateway comprising:

   an input for receiving communications packets;
   an output for outputting communications packets generally in real time with respect to receipt thereof; and
   a packet collection agent receiving packets from said input in accordance with criteria established by said policy manager; and
   a content inspector operated by the packet collection agent for inspecting said collection of packets and being operative to prevent supply of at least one packet of a collection of packets to said output when said collection of packets includes undesirable content.

9. A gateway according to claim 8 and wherein said at least one packet is the last packet of a file.

10. A gateway according to claim 8 and wherein a policy manager determines criteria whereby not all files are inspected.

11. A method for protecting a computer from malicious content comprising the steps of:

    determining criteria for collection and inspection of a collection of packets;
    receiving packets from among the collection of packets in accordance with the criteria;
    inspecting the packets in accordance with the criteria;
    preventing output of at least one packet but not all packets of a collection of packets when the collection of packets includes undesirable content in accordance with the criteria; and
    outputting packets other than the at least one packet generally in real time with respect to receipt thereof.

12. A method according to claim 11 and wherein said at least one packet is the last packet of a file.

13. A method according to claim 11 and wherein a policy manager determines criteria whereby not all files

are inspected.

14. A method according to claim 11 and wherein a packet collection agent inspects all packets of files that are to be inspected.

15. A method according to claim 11 and wherein a packet collection agent operates plural content inspectors simultaneously.

16. A method according to claim 11 and wherein a policy manager determines criteria whereby some types of files are not released even without inspection by a content inspector.

17. A gateway according to claim 11 and wherein a packet collection agent operates on Internet but not on Intranet traffic.

FIG. 1A

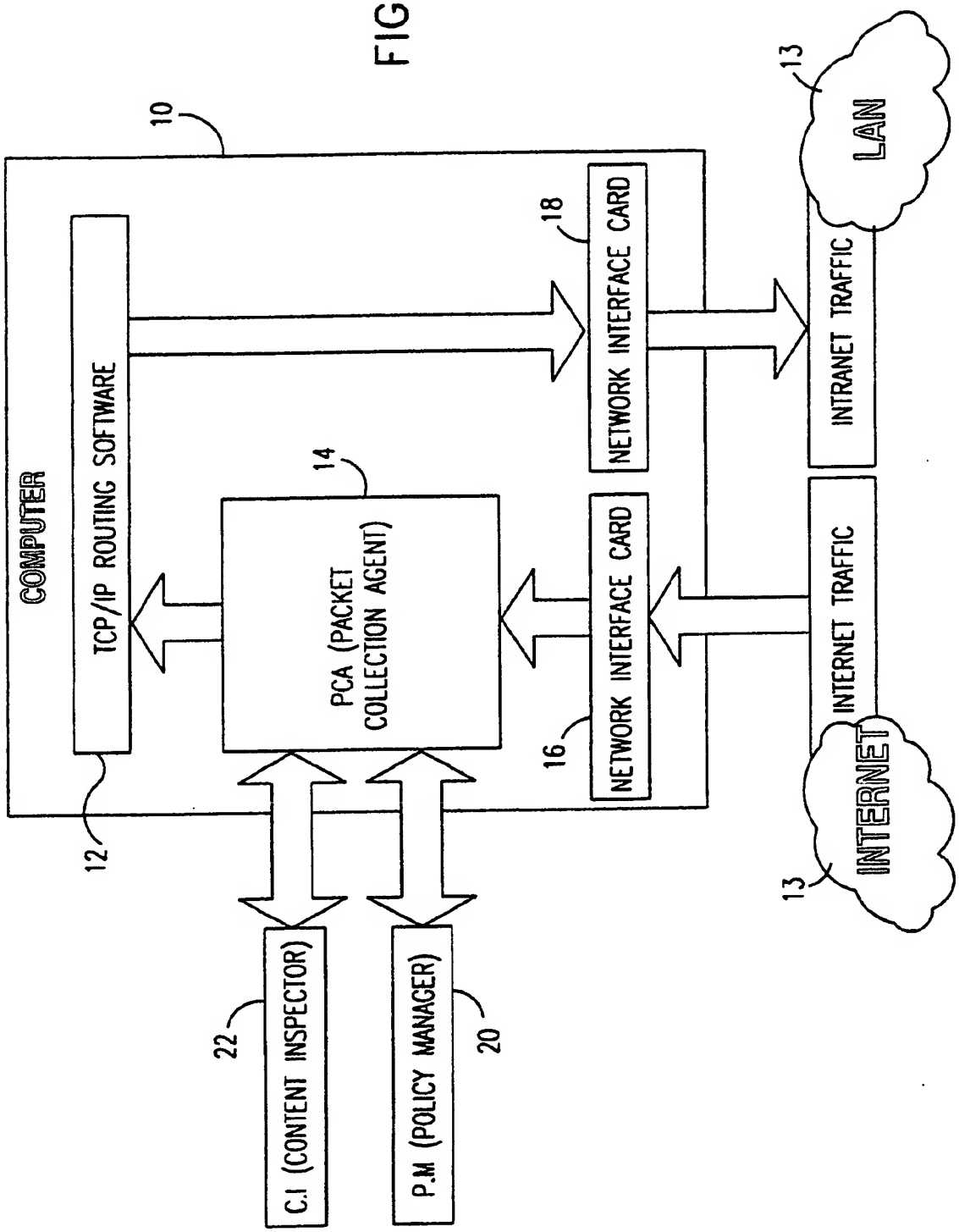


FIG. 1B

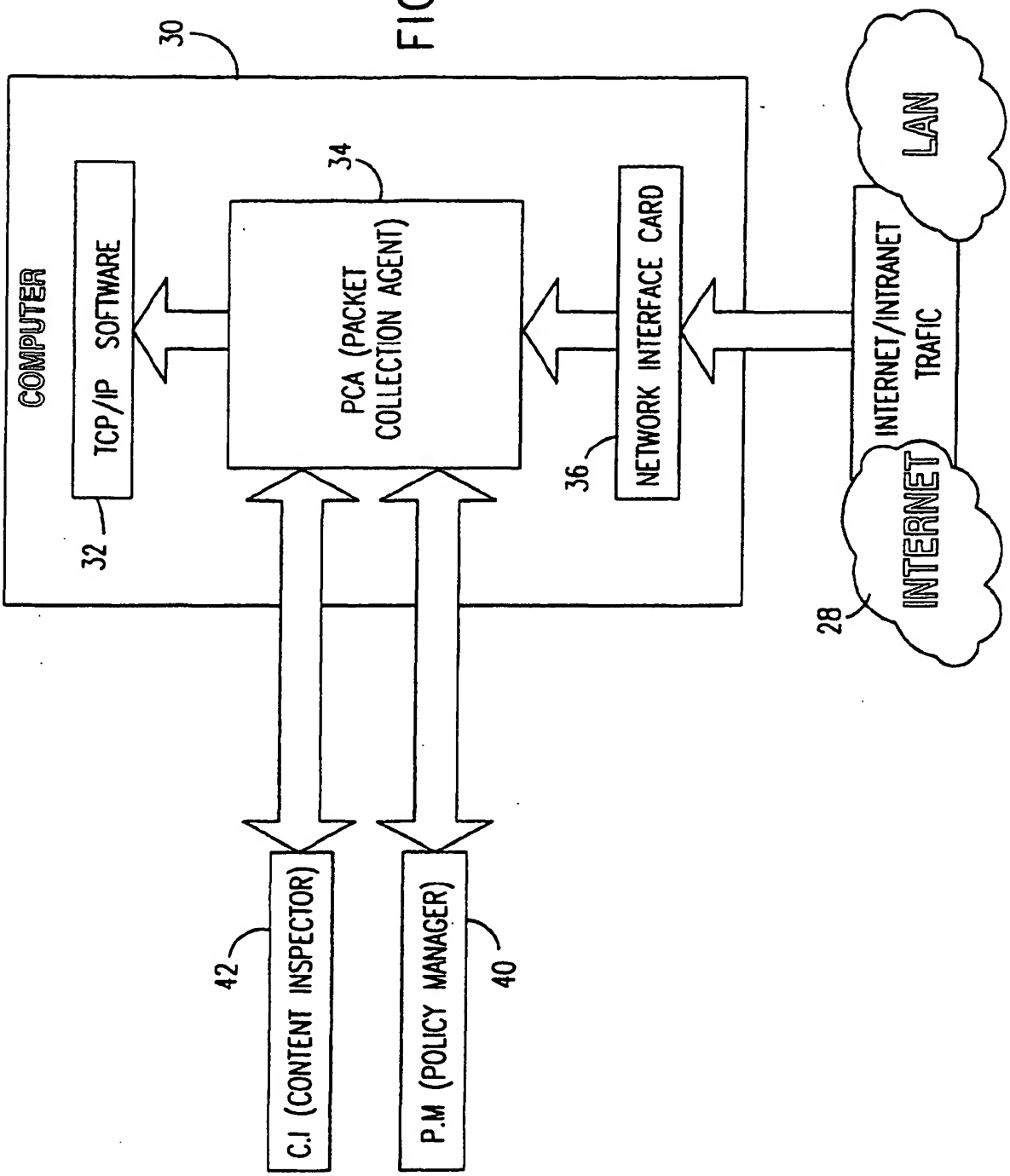


FIG. 2

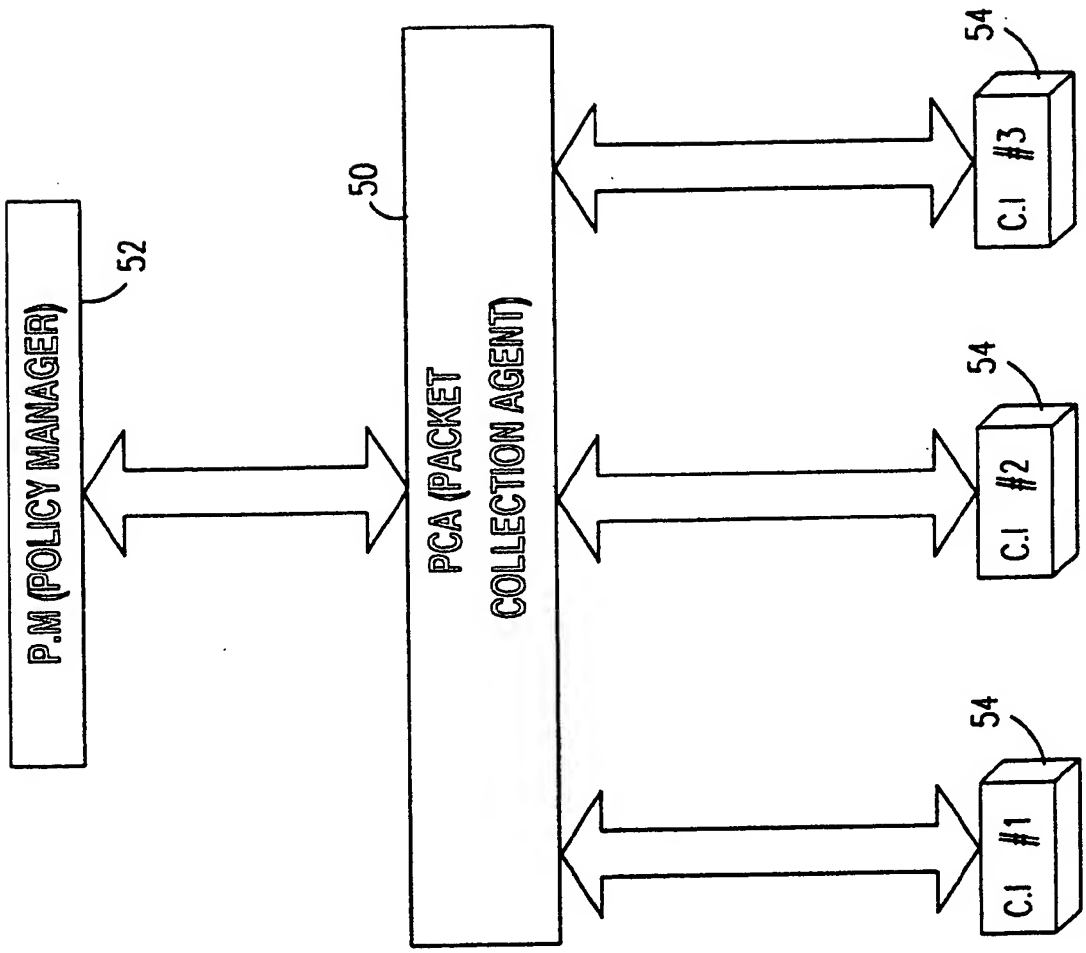
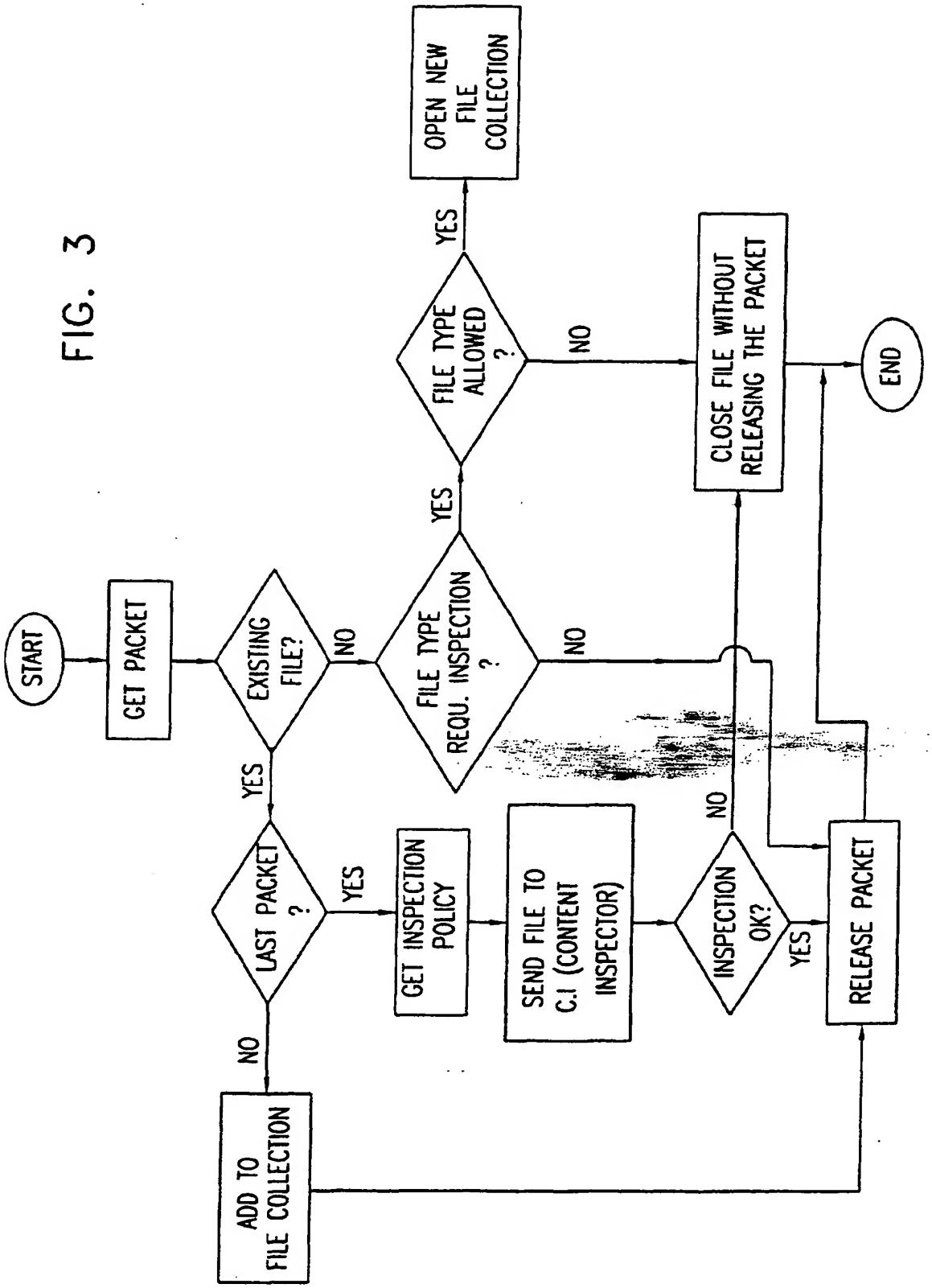


FIG. 3



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 10 2150

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 00 00879 A (HANNEL CLIFFORD L ;INTERNET DYNAMICS INC (US); LIPSTONE LAURENCE R) 6 January 2000 (2000-01-06)	1-4,8-14	H04L29/06 G06F1/00
Y	* abstract * * page 70, line 15 - line 28 * * page 76, line 28 - page 77, line 2 *	5-7, 15-17	
X	WO 97 39399 A (TREND MICRO INC ;CHEN EVA (US)) 23 October 1997 (1997-10-23)	1,3-8,10	
Y	* abstract * * page 4, line 5 - page 5, line 25 * * page 9, line 22 - line 32 * * page 11, line 27 - page 15, line 21 * * page 15, line 22 - page 18, line 28 * * page 21, line 23 - line 30 * * page 28, line 26 - page 29, line 2 *	5-7, 15-17	
L	US 6 088 803 A (BAKSHI BIKRAM SINGH ET AL) 11 July 2000 (2000-07-11) * abstract * * column 3, line 11 - column 4, line 49 * * column 5, line 44 - column 6, line 37 *	1,2,8,9, 11,12	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	13 August 2003	Horn, M.P.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 122 932 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
08.10.2003 Bulletin 2003/41

(43) Date of publication A2:
08.08.2001 Bulletin 2001/32

(21) Application number: **01102150.8**

(22) Date of filing: **01.02.2001**

(51) Int Cl.[7]: **H04L 29/06**, G06F 1/00

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **04.02.2000 US 498093**

(71) Applicant: **Aladdin Knowledge Systems Ltd.**
Tel Aviv 67211 (IL)

(72) Inventors:
- **Margalit, Dany**
  Ramat Gan 52223 (IL)
- **Gruper, Shimon**
  Kiryat Haim 26307 (IL)

(74) Representative: **Modiano, Guido, Dr.-Ing. et al**
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
80469 München (DE)

(54) Protection of computer networks against malicious content

(57) A gateway including an input for receiving communications packets, an output for outputting communications packets generally in real time with respect to receipt thereof, a policy manager (20) determining criteria for collection and inspection of a collection of packets and a packet collection agent (14) receiving packets from the input in accordance with criteria established by the policy manager and including a content inspector (22) inspecting the collection of packets in accordance with criteria established by the policy manager and being operative to prevent supply of at least one packet of a collection of packets to the output when the collection of packets includes undesirable content in accordance with the criteria established by the policy manager.

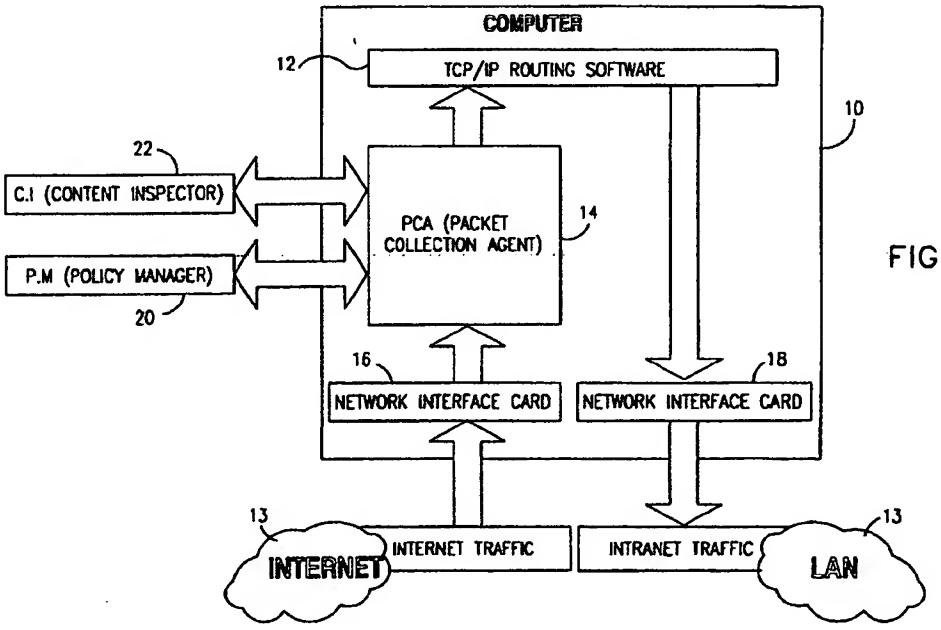


FIG. 1A

EP 1 122 932 A3

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 10 2150

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

13-08-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0000879 A	06-01-2000	US 6408336 B1	18-06-2002
		AU 733109 B2	10-05-2001
		AU 6452798 A	29-09-1998
		EP 0966822 A2	29-12-1999
		WO 9840992 A2	17-09-1998
		WO 0000879 A2	06-01-2000
		AU 762061 B2	19-06-2003
		AU 4838699 A	17-01-2000
		EP 1105809 A2	13-06-2001
		TW 448387 B	01-08-2001
WO 9739399 A	23-10-1997	US 5889943 A	30-03-1999
		AU 2556697 A	07-11-1997
		EP 0954794 A2	10-11-1999
		JP 2000517440 T	26-12-2000
		WO 9739399 A2	23-10-1997
US 6088803 A	11-07-2000	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82